GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE

A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES

1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org

GUIDELINES AVAILABLE AT:
http://www.constitutionproject.org/pdf/
Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf

I. Core Principles Governing the Creation and Design of Public Video Surveillance Systems

1. Create a public video surveillance system only to further a clearly articulated law enforcement purpose.

2. Create permanent public video surveillance systems only to address serious threats to public safety that are of indefinite duration.

3. Ensure that public video surveillance systems are capable of effectively achieving their articulated purposes.

4. Compare the cost of a public video surveillance system to alternative means of addressing the stated purposes of the system.

I. Core Principles Governing the Creation and Design of Public Video Surveillance Systems (Continued)

5. Assess the impact of a public video surveillance system on constitutional rights and values.

6. Design the scope and capabilities of a public video surveillance system to minimize its negative impact on constitutional rights and values.

7. Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system.

8. Ensure that the decision to create a public video surveillance system, as well as major decisions affecting its design, are made through an open and publicly accountable process.

II. Publicly Accountable Procedures for Establishing Public Video Surveillance Systems

1. For permanent or long-term public video surveillance systems, conduct a civil liberties impact assessment and overall cost-benefit analysis through a public deliberative process that includes community input.
2. For temporary public video surveillance systems, demonstrate to a neutral magistrate that the system has no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose.

III. Principles and Rules for Use of Public Video Surveillance Systems

1. Once a public video surveillance system is authorized, no additional approval is necessary to use the capabilities of the system for “observation.”

2. “Record” footage from public video surveillance systems only to the extent necessary to further the system’s stated purposes.

3. Under most circumstances, individuals may be “tracked” or “identified” by a public video surveillance system only pursuant to a warrant: (a) law enforcement must obtain a warrant prior to using a public video surveillance system to track or identify an individual; (b) law enforcement must obtain a warrant prior to using a “watch list” to automatically identify individuals, except when using a federal anti-terrorism watch list.

III. Principles and Rules for Use of Public Video Surveillance Systems (Continued)

4. A public video surveillance system may be used for legitimate law enforcement purposes other than its original purpose, subject to certain restrictions: (a) no additional approval is required for incidental use of the system; (b) law enforcement must obtain administrative approval for secondary use of “pre-archival” stored video surveillance footage; (c) law enforcement must obtain a warrant for secondary use of “archival” stored video surveillance footage.

5. Employ technological and administrative safeguards to reduce the potential for misuse and abuse of the system: (a) provide safeguards for use of stored video surveillance data; (b) provide safeguards for personnel with access to a public video surveillance system; (c) provide public notice of surveillance where appropriate.

III. Principles and Rules for Use of Public Video Surveillance Systems (Continued)

6. Prohibit, to the extent possible, sharing of public video surveillance data with third parties, including private litigants, and restrict sharing with other governmental entities.

7. Establish mechanisms to protect the rights of identifiable individuals captured on video surveillance data.

8. Apply to any law enforcement use of privately collected video surveillance data the same standards that apply to public video surveillance data.

9. Provide appropriate remedies for those harmed by misuse or abuse of public video surveillance systems.

The Constitution Project's Video Surveillance Guidelines and The Fair Information Practice Principles

1. **Principle of Transparency**

   a. Use publicly accountable procedures to establish any permanent video surveillance system. Ensure that the decision to create a public video surveillance system, as well as major decisions affecting its design, are made through an open and publicly accountable process. Guidelines pp. 20- 23. Model Legislation Sections 202-209.

   b. Use signage to alert public to the presence of cameras. Guidelines p. 32. Model Legislation Section 332.

2. Principle of Individual Participation

a. Include an opportunity for public comment as part of procedures to establish any permanent video surveillance system. Guidelines pp. 20-23. Model Legislation Sections 205-207.

b. Individuals should have the right to request a report listing instances in which they appear in video footage and are identified by name; and should have a reasonable opportunity to amend their data if it contains errors. Guidelines p. 34. Model Legislation Section 306.

3. Principle of Purpose Specification

a. The first “core principle” of the Guidelines for Public Video Surveillance is that communities should “create a video surveillance system only to further a clearly articulated law enforcement purpose.” Guidelines p. 15. Model Legislation Sections 204, 208.

b. Communities should design systems to ensure that they are capable of effectively achieving their articulated purposes. Guidelines p. 17. Model Legislation Sections 202-209.

4. Principle of Minimization

a. Determine whether video surveillance is needed to accomplish the community's law enforcement purpose. Compare the cost of a public video surveillance system to alternative means of addressing the stated purposes of the system. Alternatives to consider include additional police officers and improved street lighting. Guidelines pp. 17-18. Model Legislation Sections 202-209.

b. Design the scope and capabilities of a public video surveillance system to minimize its negative impact on constitutional rights and values. These include privacy, freedom of speech, freedom of association, and equal protection. Guidelines pp. 18-20. Model Legislation Sections 202-209.

4. **Principle of Minimization** (Continued)

c. Examples:

i. A camera installed to monitor city hall for potential terrorist threats should not be able to pan, tilt, and zoom to view into the windows of the apartment building next door.

ii. A camera installed to monitor a dangerous intersection for traffic accidents does not need facial recognition capabilities to identify passengers in the stranded cars.

iii. If political demonstrations are filmed to assess whether officers are needed on the scene to handle any outbreaks of violence, any footage of non-violent political activity should not be retained.

5. Principle of Use Limitation

a. Prohibit, to the extent possible, sharing of public video surveillance data with third parties, including private litigants, and restrict sharing with other governmental entities. Guidelines p. 33. Model Legislation Sections 321-324.

b. Require additional specific approvals to use more intrusive technologies such as automatic tracking or automatic identification. Guidelines pp. 27-29. Model Legislation Sections 302-310.

c. Require additional specific approvals to use stored footage for a “secondary purpose:” a law enforcement purpose other than the original purpose for which the systems was designed and installed. Guidelines pp. 29-30. Model Legislation Sections 317-318.

6. Principle of Data Quality and Integrity

a. Provide safeguards for use of stored video surveillance data such as requiring digital watermarks. Guidelines p. 31. Model Legislation Section 325.

b. Provide safeguards for personnel with access to a public video surveillance system including requiring training for all personnel with access to the system. Guidelines p. 32. Model Legislation Sections 326-327.

c. Establish a data retention policy under which recorded footage lacking evidentiary value will be routinely destroyed after a specified time. Guidelines p. 26. Model Legislation Sections 313-319.

7. Principle of Security

a. Provide appropriate sanctions against misuse and abuse of public video surveillance systems as well as remedies for those harmed by such misuse or abuse. Guidelines pp. 35-36. Model Legislation Sections 218-219, 328-331.

b. Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system. For example, use “digital masking” technologies to hide the identities of individuals who were incidentally captured on camera, but who are irrelevant to any investigation. Guidelines p. 31. Model Legislation Section 325.

8. Principle of Accountability and Auditing

a. Conduct periodic audits – generally at least every two years – to assess the system's effectiveness, its impact on the community, and its adherence to the system's stated primary purpose. Guidelines p. 31. Model Legislation Sections 213-217.

b. Apply to any law enforcement use of privately collected video surveillance data the same standards that apply to public video surveillance data. Guidelines p. 35. Model Legislation Section 333.

Members of the Liberty and Security Initiative Endorsing the Constitution Project's *Guidelines for Public Video Surveillance**

Co-Chairs

David Cole—Professor of Law, Georgetown University Law Center

David Keene—Chairman, American Conservative Union

Members

Floyd Abrams, Esq.—Partner, Cahill Gordon & Reindel LLP

Dr. Azizah Y. al-Hibri—Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

David Lawrence, Jr.—President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Stephen M. Lilienthal—Director, Center for Privacy and Technology Policy, Free Congress Foundation

(Members Continued)

The Honorable Bob Barr—former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union; Chairman of Patriots to Restore Checks and Balances; practicing attorney; Consultant on Privacy Matters for the ACLU

John J. Curtin, Jr.—Bingham McCutchen LLP; former President, American Bar Association

The Honorable Mickey Edwards—Director, Aspen Institute-Rodel Fellowships in Public Leadership; Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton; former Member of Congress (R-OK); former Chairman, House of Representatives Republican Policy Committee

Dr. Morton H. Halperin—Director of U.S. Advocacy, Open Society Institute; Senior Vice President, Center for American Progress

Kate Martin—Director, Center for National Security Studies

John Podesta—President and CEO, Center for American Progress; White House Chief of Staff, Clinton Administration

(Members Continued)

•**The Honorable William S. Sessions**—former Director, Federal Bureau of Investigation; former Chief Judge, United States District Court for the Western District of Texas

John Shore—Founder and President, noborg LLC; former Senior Advisor for Science and Technology to Senator Patrick Leahy

John F. Terzano—President, The Justice Project

John W. Whitehead—President, The Rutherford Institute

Roger Wilkins—Clarence J. Robinson Professor of History and American Culture, George Mason University

** Organizational information is listed for identification purposes only.*